

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Missouri

In the Matter of the Search of )

limitlessholdingsllc@gmail.com, WHICH IS STORED AT )  
PREMISES CONTROLLED OR OPERATED BY )  
GOOGLE AT 1600 AMPHITHEATRE PARKWAY  
MOUNTAIN VIEW CALIFORNIA 94043.

No. 4:23 MJ 8129 SRW

**FILED UNDER SEAL**

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY  
RELIABLE ELECTRONIC MEANS

## APPLICATION FOR A SEARCH WARRANT

I, Brock Gale, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

**See Attachment A**

located in the Northern District of California, there is now concealed

**See Attachment B**

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*

*Offense Description*

Title Section

Title 18, United States Code, Sections 922(g)(1) (felon in possession of a firearm); 922(d) (knowingly giving a firearm to a felon); 922(k) (knowingly possessing/manufacturing a short-barreled rifle); and 932 (knowingly purchasing or conspiring to purchase any firearm for a prohibited person)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the following is true and correct.

**BROCK GALE** Digitally signed by BROCK GALE  
Date: 2023.05.18 16:21:03 -05'00'

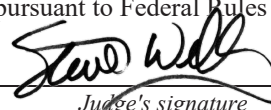
*Applicant's signature*

Brock Gale, SA, ATF

*Printed name and title*

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: May 19, 2023

  
*Judge's signature*

City and State: St. Louis, Missouri

Honorable Stephen R. Welby, U.S. Magistrate Judge

*Printed name and title*

AUSA: Jennifer Szczucinski

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF )  
INFORMATION ASSOCIATED WITH )  
limitlessholdingsllc@gmail.com THAT IS )  
STORED AT PREMISES CONTROLLED  
BY GOOGLE AT 1600 AMPHITHEATRE  
PARKWAY MOUNTAIN VIEW  
CALIFORNIA 94043.

No. 4:23 MJ 8129 SRW

**FILED UNDER SEAL**

SIGNED AND SUBMITTED TO THE COURT FOR  
FILING BY RELIABLE ELECTRONIC MEANS

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Brock Gale, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with a certain account that is stored at premises controlled by Google, an email provider headquartered at [[**PROVIDER ADDRESS**]] (hereinafter referred to as “the Provider”). The information to be searched is described in the following paragraphs and in Attachment A. The search warrant would require the Provider to disclose to the United States copies of the information (including the content of communications) further described in Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”), and have been since January 2018. I am currently assigned to the Kansas City Field Division, St. Louis Group IV Field Office. I am tasked with investigating violations of the federal arson, explosives, controlled substances, violent crime and firearms laws, among others. I

have successfully completed the Criminal Investigator Training Program (CITP) and the ATF National Academy Special Agent Basic Training (SABT) at the Federal Law Enforcement Training Center. Prior to ATF I was employed as a Police Officer for the City of Bridgeton for over six years. During my tenure with the ATF, I have participated in numerous investigations, to include burglaries of gun stores, straw purchases, and illegal firearm possession. I am familiar with and have used normal methods of investigation, including, but not limited to, visual and electronic surveillance, questioning of witnesses and defendants, the use of search and arrest warrants, the use of informants, the use of pen registers, the utilization of confidential sources and undercover agents, and the use of court-authorized wire and electronic intercepts.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 922(g)(1) (felon in possession of a firearm); 922(d) (knowingly giving a firearm to a felon); 922(k) (knowingly possessing/manufacturing a short-barreled rifle); and 932 (knowingly purchasing or conspiring to purchase any firearm for a prohibited person) (hereinafter referred to as “the subject offenses”) have been committed by **DENNIS LATOUR** and **JENNIFER KEEGAN**, and others known and unknown. There is also probable cause to search the location described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **LOCATION TO BE SEARCHED**

5. The location to be searched is:  
  
limitlessholdingsllc (hereinafter referred to as the “Subject Account”) located at limitlessholdingsllc@gmail.com, described in Attachment A. The items to be reviewed and seized are described in Attachment B.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **BACKGROUND CONCERNING EMAIL**

7. In my training and experience, I have learned that the Provider provides a variety of on-line services, including electronic mail (“email”) access, to the public. The Provider allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with the Provider. During the registration process, the Provider asks subscribers to provide basic personal information. Therefore, the computers of the Provider are likely to contain stored electronic communications (including retrieved and unretrieved email for the Provider subscribers) and information concerning subscribers and their use of the Provider services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

8. Subscribers can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the Provider. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address

information can help to identify which computers or other devices were used to access the email account.

11. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

12. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the

chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

13. In general, an email that is sent to the Provider is stored in the subscriber's "mail box" on the Provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the Provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for an extended period of time and, in some circumstances, indefinitely.

### **BACKGROUND CONCERNING GOOGLE**

14. I have learned the following about Google:

a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using the Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Android ID, Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated



Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

v. *Cookie Data.* Google uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user’s computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

vi. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google’s websites). Google also retains information regarding accounts registered from the same IP address.

vii. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

viii. *Preserved and backup records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

15. In addition, Google maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, which typically include the following:

a. *Google Drive content.* Google provides users with a certain amount of free “cloud” storage, currently 15 gigabytes, through a service called “Google Drive” (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content “in the cloud,” that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive.

c. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

d. *Google Calendar.* Google provides users with an online calendar, in which they

can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

f. *Location History data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device’s most recent location data in connection with a Google account.

g. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Google Profile.* Google allows individuals to create a Google profile with certain identifying information, including pictures.

i. *Google Plus.* Google hosts an Internet-based social network. Among other things,

users can post photos and status updates and group different types of relationships (rather than simply “friends”) into Circles. In addition, Google has a service called PlusOne, in which Google recommends links and posts that may be of interest to the account, based in part on accounts in the user’s Circle having previously clicked “+1” next to the post. PlusOne information therefore provides information about the user of a given account, based on activity by other individuals the user has entered in the user’s Circle.

j. *Chrome Browser and Search History.* Google stores information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in the Google Internet search engine available at <http://www.google.com> (and variations thereof, including <http://www.google.ru>), and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

k. *Advertising Data.* Google also stores advertising data, including information regarding unique advertising IDs associated with the customer, devices used to access the account, application IDs, advertising cookies, Unique Device Identifiers (UDIDs), payment information, ads clicked, and ads created.

l. *YouTube Data.* Google owns the video-streaming service YouTube and maintains records relating to YouTube accesses and data posted by the user

16. Therefore, the computers of Google and are likely to contain stored electronic communications (including retrieved and unretrieved email) for Google subscribers and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training

and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. As explained above, Google subscribers can also store with the providers files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

18. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

19. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. As explained herein, information stored in connection with a Google account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to

commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement)

**PROBABLE CAUSE**

21. The United States, including ATF, is conducting a criminal investigation of JENNIFER KEEGAN and convicted felon DENNIS LATOUR regarding the commission of the subject offenses. From February of 2023 to May of 2023, SA Gale has been investigating the suspected straw purchasing and attempted straw purchasing of approximately 20 firearms purchased by KEEGAN and LATOUR from 5 different locations.

22. LATOUR is a convicted felon, having prior convictions for: Case No. 4:12-CR-00231 CDP - Bank Fraud, Identity Theft, and Wire Fraud; Case Number 4:15-CR-241 RLW-6 - Conspiracy to Launder Money and Money Laundering; Case No. 11SL-CR04774-01 - Unlawful Merchandise Practice and Passing a Bad Check; Case No. 12SL-CR00047-01 - Stealing over \$25,000, and additional stealing/theft convictions prior to 2010.

23. On February 24, 2023, an online order was placed through [www.gunprime.com](http://www.gunprime.com) for a Barrett, model M82A1, .50 caliber rifle, two boxes of 10 rounds of .50 BMG caliber ammunition and one Barrett, model M82A1 10 round magazine. The credit card provided was XXXX-XXXX-XXXX-2055 with name "Jennifer Keegan." The original name on the online order was Dennis Latour, however LATOUR then called [gunprime.com](http://gunprime.com) from telephone number (314) 600-6551 and advised he wished to switch the name on the order to KEEGAN. Additionally, LATOUR requested overnight delivery and agreed to pay the \$300.00 fee.

The information listed on the invoice was:

Jennifer Keegan  
12429 Nicholas Ln.,  
Saint Louis, MO 63131  
United States  
3146006551  
limitlessholdingsllc@gmail.com (the **Subject Account**)

24. The representative at gunprime.com advised due to the price of the order they declined the transaction and advised LATOUR the transaction would only be completed if a certified check was delivered. Employees performed an online public records inquiry and learned LATOUR was likely a felon.

25. In March of 2023, after being denied the firearm transaction by gunprime.com, LATOUR contacted the owner (J.S.) of JS Gunworks, a Federal Firearms Licensee. JS Gunworks is located at 3697 Broad St., Saint Charles, MO 63301. LATOUR informed J.S. of the denied firearms transaction and asked J.S. to complete the order through gunprime.com. LATOUR advised J.S. that gunprime.com would not complete the order if anyone involved in the denied transaction was involved with attempting to purchase the Barret, .50 caliber rifle. LATOUR sent J.S. a screenshot of the invoice from gunprime.com and the cancelled payment message from gunprime.com to LATOUR. The screenshot appears to be from a cellular phone, and displays a response from what appears to be LATOUR after the payment was voided stating, "Are you kidding us? So if we mail a check you hold it for 10 days and we."

26. At LATOUR's request, J.S. purchased the firearm from gunprime.com, to be shipped to J.S. and transferred to LATOUR and KEEGAN upon its arrival.

27. On March 1, 2023, KEEGAN and LATOUR arrived at JS Gunworks and purchased the Barrett, 82A1-CQ, .50 BMG caliber rifle, and an Aero Precision, X15, multi caliber rifle with



cash. KEEGAN completed the Firearms Transaction Record (ATF Form 4473). After this purchase, LATOUR sent J.S. photos of the Barrett rifle and inquired if the scope was mounted properly. The photos show the Barrett rifle sitting on a table with various tools, in what appears to be a large garage/airplane hangar. In one of the photos, the tag is still affixed to the rifle, with the serial number clearly visible.



*Barrett, 82A1-CQ, .50 BMG caliber rifle, SN: AA014535*

28. J.S. advised he first met KEEGAN and LATOUR at a gun show on December 10, 2022. KEEGAN completed ATF Form 4473 and purchased a JS Gunworks JSG-15, .50 Beowulf caliber rifle and a second firearm from J.S.'s private collection, which was not documented on the Form 4473. KEEGAN used cash to purchase the firearms. J.S. recalled both KEEGAN and LATOUR discussing buying firearms from other dealers and observed LATOUR and KEEGAN both carrying items out of the gun show.



*JS Gunworks JSG-15, .50 Beowulf caliber rifle purchased by KEEGAN/LATOUR*



*Red and black rifle purchased by KEEGAN/LATOUR. Pistol in above picture is not relevant.*

29. After this first purchase, J.S. would routinely exchange text messages and phone calls with LATOUR. J.S. advised he and LATOUR discussed various things, including building custom firearms. During these conversations, J.S. agreed to build a custom firearm for LATOUR. On February 24, 2023, LATOUR and KEEGAN arrived at JS Gunworks. KEEGAN completed Form 4473 and purchased the firearm with cash. The firearm is described as a JS Gunworks, JSG-15, 5.56 caliber rifle, with a Fightlite upper receiver which is capable of firing belt fed or magazine fed.



30. During conversations with LATOUR, LATOUR mentioned he was a pilot and works or has an office at Creve Coeur or Chesterfield Airport. J.S. stated LATOUR and KEEGAN are always together and believes they are married. All of the transactions completed with LATOUR and KEEGAN have been cash transactions.

31. On March 4, 2023, KEEGAN and LATOUR went to Bass Pro Shop, located at 1365 South 5<sup>th</sup> St., Saint Charles, MO 63301, within the Eastern District of Missouri. While at Bass Pro, KEEGAN completed ATF Form 4473 and purchased a Umarex/HK Inc., MP5, .22 caliber rifle and a Riley Defense, RAK-47, 7.62x39mm caliber rifle.

32. SA Gale seized and reviewed a copy of the surveillance video. For the majority of the transaction KEEGAN stood at the firearm counter handling the transaction. LATOUR meandered about and occasionally stood next to KEEGAN. LATOUR engaged in conversation with the store employee and inspected the firearms being purchased by KEEGAN. At one point during the video, an employee handed LATOUR what appears to be a long rifle from the display wall. LATOUR handled the suspected firearm for a brief period and returned it to the employee. Prior to LATOUR exiting the store, LATOUR made a purchase for a Magpul rail light mount, which is designed to secure a light to a firearm. LATOUR and KEEGAN exited the store, each of them holding a firearm.

33. On March 21, 2023, KEEGAN and LATOUR went to Bass Pro Shops Outdoor World, located at 1 Bass Pro Drive, Springfield, MO 65807. KEEGAN completed ATF Form 4473 and purchased five firearms: Kimber, Micro 9 Rapide, 9mm luger caliber pistol, Heckler & Koch, Inc., MR762 A1, 7.62 caliber rifle, Kimber, Aegis Elite Custom, 9mm luger caliber pistol, Christensen Arms, CA-10 G2, 6.5 mm Creedmoor caliber, Derya Arms / AP INTL, VR80, 12 gauge caliber shotgun.

34. SA Gale seized and reviewed a copy of the surveillance video which showed the following:

35. KEEGAN and LATOUR arrived at Bass Pro together, in a black Alpha Romeo SUV with LATOUR driving.

36. KEEGAN and LATOUR entered the Fine Gun Room and perused items. While KEEGAN was on one side of the room, LATOUR made contact with an employee and pointed to firearms within a case. The employee handed LATOUR multiple different firearms, which LATOUR manipulated and then returned to the employee.

37. Thereafter, KEEGAN and LATOUR went to the firearms counter for over an hour. During this time period LATOUR engaged in conversation with an employee working behind the counter. LATOUR handled approximately twelve different firearms, usually outside KEEGAN's presence. At one point, LATOUR had two AR-style rifles on the counter; LATOUR utilized a cellular phone while examining the firearms and showed the screen of his phone to the employee. Once KEEGAN returned to LATOUR's side, she never touched the firearms. Ultimately, LATOUR gestured toward the firearms, then the employee took the firearms to an area where KEEGAN and LATOUR would eventually complete the transaction for all five firearms.



*LATOUR utilizing his cell phone while handling two firearms.*

38. On March 22, 2023, KEEGAN went to Eagle Armory, located at 1908 E Chestnut Expy, Springfield, MO 65802. KEEGAN completed ATF Form 4473 and purchased a Heckler & Koch / HK Inc., SP5, 9mm caliber pistol. Employees recalled KEEGAN being accompanied by a male, however surveillance video was not obtainable.

39. On April 4, 2023, KEEGAN and LATOUR went to Midwest Gun Works Inc., located at 1101 Mason Circle Dr. S, Pevely, MO 63070. KEEGAN completed ATF Form 4473 and purchased the following three firearms: IWI, Tavor X95 XB18, 5.56 caliber rifle, Kriss USA, Vector SDP G23, 10mm caliber pistol, and a Fightlite, SCR, multi caliber pistol. The firearms were made via three separate online orders. The following purchaser information was provided as part of the online orders:

Jennifer Keegan  
12429 Nicholas Ln  
Saint Louis MO 63131-3625  
US  
3143038034

40. SA Gale reviewed the surveillance video and interviewed the Midwest Gun Works store manager and learned the following:

41. LATOUR and KEEGAN arrived at the store together, with LATOUR driving a black/red Toyota FJ Cruiser with off road accessories.

42. LATOUR entered the store carrying a black soft sided case and removed a silver pistol from the case. LATOUR then exchanged magazines that were purchased via an online sale to KEEGAN.





*(left) LATOUR holding what appears to be a Kimber, Micro 9mm pistol at Midwest Gunworks. (right) exemplar photo of a Kimber, Micro 9mm pistol from the Kimber website located at <https://www.kimberamerica.com/micro-9-rapide-frost>.*

43. The store employee showed LATOUR and KEEGAN the three firearms and both KEEGAN and LATOUR inspected them. KEEGAN purchased additional items, including magazines and Kriss Vector folding stock. KEEGAN completed ATF Form 4473 and LATOUR handled the Kriss firearm and the Kriss Vector folding stock. LATOUR appeared to discuss attaching the stock to the firearm with the employee. KEEGAN showed no interest in the stock or how it attached to the firearm. LATOUR utilized a cellular phone to watch a video in reference to the firearm. Employees brought LATOUR a second stock which, LATOUR and the employee manipulated with the firearm. Affixing the stock to the Kriss pistol, would convert this firearm into a short barreled rifle, in violation of Title 18, United States Code, Section 922(k).



*LATOUR removing the Kriss firearm from the case.*



*LATOUR utilizing a cellular phone.*

44. During the interaction, LATOUR removed a credit/debit card from his wallet and gave it to the employee to pay for the difference owed as the new stock LATOUR selected was more expensive. The last four digits of the credit card utilized for all of the transactions at Midwest Gunworks was 2055. It should be noted the credit card originally utilized to attempt to purchase the Barrett, .50 caliber rifle from gunPrime.com was XXXX-XXXX-XXXX-2055.

45. Relative to the Subject Account, the Missouri Secretary of State reflects that LATOUR provided a Missouri Business Filing for Limitless Holding LLC on February 27, 2023. According to records, LATOUR is the registered agent and organizer for Limitless Holding LLC, with a principal office address of 1096 Mersey Bend Dr., Apt. G, Saint Louis, MO 63129. LATOUR provided the Subject Account as the email for Limitless Holdings LLC.

46. On May 17, 2023, a preservation request was delivered to Google for the **Subject Account**.

### **CONCLUSION**

47. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on the Provider. Because the warrant will be served on the Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

48. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,



destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

**BROCK  
GALE**

Digitally signed by  
BROCK GALE  
Date: 2023.05.18  
16:20:47 -05'00'

---

Brock Gale  
Special Agent  
ATF

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41, on May 19\_\_\_\_\_, 2023

  
\_\_\_\_\_  
The Honorable Stephen R. Welby  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with limitless Holdings LLC@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 AMPHITHEATRE PARKWAY MOUNTAIN VIEW CALIFORNIA 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The content of all communications sent to or from the account (including through Gmail, Google Hangouts (including videos), and otherwise), stored in draft form in the account, or otherwise associated with the account, including all message content, attachments, and header information;
- b. All address book, contact list, or similar information associated with the account;
- c. Full Google search history and Chrome browser history associated with the account;
- d. All Google Drive content;
- e. All bookmarks maintained by the account;
- f. All services used by the account;
- g. All subscriber and payment information, including full name, e-mail address (including any secondary or recovery email addresses), physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, telephone number, websites, screen names,

user identification numbers, security questions and answers, registration IP address, payment history, and other personal identifiers;

h. All past and current usernames, account passwords, and names associated with the account;

i. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;

j. All YouTube data associated with the account;

k. All transactional records associated with the account, including any IP logs or other records of session times and durations;

l. Any information identifying the device or devices used to access the account, including a device serial number, a GUID or Global Unique Identifier, Android ID, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the account;

m. All activity logs for the account;

n. All photos and videos uploaded to the account, including in Google Drive and Google Photos;

o. All information associated with Google Plus, including the names of all Circles and the accounts grouped into them;

p. All photos and videos uploaded by any user that have that user tagged in them;

- q. All location and maps information;
- r. All Google Voice information;
- s. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- t. All privacy settings and other account settings, including email addresses or other accounts that the account has blocked;
- u. Advertising and Device Data: All advertising data relating to the account, including, but not limited to, advertising cookies, information regarding unique advertising IDs associated with the user, any devices used to access the account, Android IDs, application IDs, UDIDs, payment information (including, but not limited to, full credit card numbers and expiration dates and PayPal accounts), ads clicked, and ads created;
- v. Linked Accounts: All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);
- w. For accounts linked by cookie, the date(s) on which they shared a cookie;
- x. For accounts linked by SMS number, information regarding whether the numbers were verified; and
- y. Customer Correspondence: All records pertaining to communications between the Service Provider and any person regarding the user or the user's account with the Service Provider, including contacts with support services, records of actions taken, and investigative or user complaints concerning the subscriber; and
- z. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of the issuance of this warrant.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 922(g)(1) (felon in possession of a firearm); 922(d) (knowingly giving a firearm to a felon); 922(k) (knowingly possessing/manufacturing a short-barreled rifle); and 932 (knowingly purchasing or conspiring to purchase any firearm for a prohibited person) (hereinafter referred to as "the subject offenses"), occurring from January 1, 2023, to May 19, 2023, or relating to DENNIS LATOUR or JENNIFER KEEGAN including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence relating to firearms possession, including the acquisition of firearms;
- (b) Information indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crimes under investigation;
- (d) The identity of the persons who created or used the account, including records that help reveal the whereabouts of such person.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be

conducted by any United States personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, analysts, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the United States and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is \_\_\_\_\_ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.



I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature